Method and System for Encryption of Optical Signals

Field of the invention

The present invention relates to a technique for encrypting signals to be transmitted via optical communication lines, for example for protecting bank information on monetary transactions from hackers.

Background of the invention

Various techniques for encrypting analog and digital information are known in the art. The main feature of techniques for encrypting digital information is converting the data transmitted as a binary sequence and presented by high and low energy levels, into another binary sequence using a predetermined key or a system of keys. Knowing the key or the system of keys and applying them to the obtained binary sequence enables decryption of the digital information, i.e., returning it to the original binary sequence. Most of the known encryption techniques utilize a deterministic approach to the coding, even those methods introducing a random element into the technique (since they actually use pseudo-random principles).

It goes without saying that an unauthorized user will be able to decrypt the intercepted data if the key is somehow uncovered i.e., will be able to find a connection between the obtained encrypted binary data and the original binary data.

Object of the invention

It is an object of the present invention to provide a novel technique of encryption suitable for signals transmitted over optical lines.

Summary of the invention

The Inventors propose using a phenomenon of chromatic dispersion in an optical fiber for encrypting information transmitted over optical transmission lines.

In other words, there is provided a method of encrypting an optical signal to be transmitted via an optical fiber communication link by causing controlled chromatic dispersion of said signal.

The fiber chromatic dispersion *(fiber dispersion)* is a result of dependence of the fiber refractive index on the signal wavelength. Since an optic signal velocity in a fiber is given by

$$V(\lambda)=\frac{c}{n(\lambda)} \qquad (1)$$

where $V(\lambda)$ is the signal velocity, c is the light velocity in vacuum and $n(\lambda)$ is the fiber refractive index, the signal velocity also depends on the signal wavelength.

Because of the final spectral width of any optical pulse signal, its different parts will propagate through the fiber with different velocities causing the pulse distortion, which will be called *the signal dispersion* in the frame of the present application. As a result of this, various effects appear. For example, such effects are mutual interference between adjacent optical pulses within the optical channel (so-called inter-symbol interference ISI), and decrease of the pulse peak power. These effects are considered harmful, and specific techniques are usually required for overcoming them.

For compensating the *fiber dispersion*, one may use fibers with the dispersion characteristics opposite to those of the standard fiber. Such fibers are usually called dispersion compensating fibers (DCF).

One alternative technique for compensating the fiber dispersion uses chirped periodic structures to create different delays between signals of different wavelengths and therefore to compensate for the fiber chromatic dispersion. This technique is presented today by the chirped fiber Bragg gratings, for example described in a Japanese patent application JP 20002 35170 A. Arrangements belonging to this technique do not create non-linear interactions, the gratings have a small size and allow creating variable compensation modules.

To the best of our knowledge, the Applicant's idea that the negative phenomenon of signal dispersion could be used as means for encryption of optically transmitted digital signals, has not been yet realized or published.

In terms of a method and a device (system), the inventive idea can be further defined as follows:

A method for encrypting an optical signal to be transmitted via an optical fiber communication link between a transmitting site and a receiving site, comprising:

obtaining an original optical signal,

at the transmission site, encrypting the original optical signal by causing a controlled chromatic dispersion thereof,

transmitting thus encrypted optical signal,

at the receiving site, providing a suitably controlled compensation of the dispersion caused at the transmission site, thereby decrypting the encrypted signal to restore the original optical signal.

Upon such an encryption, any unauthorized user will be unable to restore the intercepted signal, since the encrypted signal constitutes a chromatically distorted original signal, while both the extent and the time order of the distortion can be controlled to make the original signal unrecognizable.

The proposed method is applicable to encryption of both digital and analog optical signals carrying information.

Creating the controlled signal dispersion can be provided by means capable of affecting chromatic dispersion in the original signal, using said means in a predetermined order and combination of the affecting operations.

In the analogous manner, the suitable controlled compensation of the dispersion can be effected by means capable of compensating chromatic dispersion created at the transmission site, using said means in the predetermined order and combination. The combination and order of operations affecting chromatic dispersion of the signal at the transmitting site to encrypt it, and at the receiving site to decrypt it, can be called the encryption-decryption key.

The key is preferably a function of time. It can be based, for example, on a pseudo-random sequence known at the receiving site and the transmission site. To be properly applied for encryption and then for decryption, the key should be synchronized with the original optical signal at the transmitting site, and that synchronization should be known at the receiving site i.e., the receiving site should be synchronized with the transmitting site from the point of encryption/decryption.

There is also provided an encryption device for encrypting an optical signal to be transmitted via an optical fiber communication link, the device being capable of causing controlled chromatic dispersion of said signal.

Likewise, a decryption device for decrypting an optical signal encrypted by the encryption device should be capable of causing controlled compensation of the chromatic dispersion introduced into said signal by the encryption device.

According to yet a further aspect of the invention, there is provided a system for encryption of an original optical signal to be transmitted via an optical fiber communication link between a transmission site and a receiving site, the system comprising

- a controllable encryption device at the transmission site, capable of causing for controlled chromatic dispersion of said original signal, and
- a suitably controllable decryption device at the receiving site, capable of compensating the chromatic dispersion caused at the transmission site so as to obtain said original signal.

According to one preferred embodiment of the device (and the system), the encryption device can be implemented in the form of a so-called variable dispersion compensation module. Similarly, the decryption device can also be implemented using a similar variable dispersion compensation module.

For example, the variable dispersion compensation module may comprise a plurality of fiber sections having different dispersion characteristics and selectively connectable to the optical communication line.

Alternatively or in addition, the variable dispersion compensation unit may comprise a set of Bragg gratings.

In the system at its transmitting site, there is preferably a transmitter assembly combined from a conventional transmitter and the encryption device in the form of a variable dispersion compensation module, controlled (modulated) by some function of time called an encryption key.

Accordingly, at the receiving site of the system, there is preferably a receiver assembly comprising a conventional receiver and the decryption device controllable by a decryption key being a function of time. Knowing the key, one can synchronize the decryption device with the encryption device and set the dispersion at the receiving site to the desired function symmetric to that at the transmitting site so as to minimize the Inter Symbol Interference (ISI) and read the information properly. Otherwise the information read by the receiver will be distorted by the chromatic dispersion and a random illegible sequence will be obtained instead of the original signal.

Brief description of the drawings

The invention can be further described and illustrated with the aid of the following non-limiting drawings in which:

Fig. 1 – is a schematic block-diagram illustrating the principle of the proposed invention

Figs. 2a, 2b, 2c illustrate, using simple examples, the principle of encrypting optical information by controlling chromatic dispersion of the optical signal.

Fig. 3 - is a schematic block-diagram illustrating one embodiment of the encryption unit according to the invention.

Fig. 4 – illustrates one embodiment of implementing the inventive concept for the multi-channel optical transmission.

Detailed description of the preferred embodiments:

Fig. 1 illustrates the principle of the invention and the proposed system.

The system 10 for protected transmission of optical information comprises equipment at a transmitting site 12, equipment at a receiving site 14 and an optical link 16 connecting the sites 12 and 14. The optical link 16 basically consists of a conventional optical fiber having a particular length, but may also comprise additional network elements such as amplifiers and various passive elements. The link may also comprise OADM (Optical Add-Drop Multiplexer), and this example will be illustrated in Fig. 4.

The transmitting site equipment comprises a transmitter 18 and a dispersion encrypting device 20 which, preferably, is implemented as a controlled variable dispersion module. The transmitter 18 produces an original optical signal which is fed to the dispersion encryption device 20 and synchronized therewith. The device 20 is controlled by an encryption key which is a function of time (schematically marked 21). The encryption device changes its dispersion characteristics in the manner dictated by the key. The encrypted optical signal is a distorted original signal, which is further transmitted via the optical link 16.

The decryption device 22 receives the encrypted optical signal transmitted via the optical link 16 and applies to the signal a properly synchronized decryption key (schematically marked 23) which is also a function of time. The decryption key 23 is capable of causing the decryption device 22 to compensate the distorting action of the encryption device 20 and thus to restore the original optical signal which is finally fed to the receiver 24. Basically, the function of the decryption key 23 and the function of the encryption key 21 are symmetric relative to the axis of time.

For example, the encryption key function may include positive and negative sections which would respectively reflect periods of introducing dispersion and periods of overcompensating; the function may also be characterized by various time derivatives of the dispersion.

However, some adjustments are to be effected at the decryption device 22, taking into account noise and other artifacts introduced by the optical link 16. Such adjustments may be introduced by slightly altering the function of the decryption key, for example by adding to it a constant negative or positive bias to compensate dispersion introduced by the fiber and/or other elements of the link 16.

Figs. 2a, 2b and 2c show, how an original optical signal can be distorted by encrypting it using a simplest dispersion encryption device.

Let us consider the system 10, comprising the transmitter 18, the tunable dispersion device 20 and the optical fiber link 16 having the length of 20 km, allows changing the initial chromatic dispersion of the original signal by the device 20 in the range analogous to the dispersion of +/- 200 km of a standard fiber (negative sign refers to overcompensation of the dispersion).

Fig. 2a shows an exemplary binary sequence "1 1 0 1" produced by the transmitter 18 as an original optical signal. This sequence, would the system comprise the optical transmission link 16 directly connected to the transmitter 18, would have propagate as the sequence of pulses of the Gaussian shape. The receiver decision threshold is set in this example for the half maximum of the initial amplitude as one can see in Fig. 2a.

Fig. 2b illustrates the distorted signal which will propagate via the system if the transmitter 18 produces the same original optical signal while the variable dispersion encryption device 20 is set to introduce a constant dispersion value equivalent to +160 km (additional 160 km) of the optical fiber. In this example, the encryption key is the simplest and constitutes just a

constant value. It can be seen that the peak power of all the distorted pulses is below the threshold now, and actually, the word
"0 0 0 0" could be read instead of the original binary sequence. Without knowing how the encryption is synchronized with the signal, and which bit rate is used in the particular transmission, the encrypted information cannot be decrypted. Indeed, without knowing these factors, the decryption cannot be performed even if the decision threshold is shifted and even when the key somehow becomes known.

To restore the original optical signal, the dispersion decryption device at the receiving site should be set to (-180 km) to compensate the dispersion introduced both at the transmission site and in the fiber link having the length of 20 km, and be synchronized with the transmitting site.

Fig. 2c presents another example of a simple encryption key. The distorted signal is shown, obtained if the dispersion encryption device is set to a constant dispersion which is equivalent to the dispersion value (-200km), i.e. which would be obtained upon compensation of dispersion which could be introduced by an optical fiber having the length of 200 km. In this case the peak powers are very close to the decision threshold and practically a random word will be obtained because of the system noise and other impairments.

For decrypting the encrypted data, the receiving site should be arranged so that, beginning from a specific moment, start introducing the dispersion having the value equivalent to about (+180 km).

It is understood that in practice, more complex encryption/decryption keys can be used, comprising time periods of artificially introduced dispersion having various values and signs.

Fig. 3 illustrates one exemplary schematic embodiment 26 of the dispersion encryption device which is based on a controlled variable dispersion module. The module, in this example, comprises a number of fiber sections (Fiber 1, Fiber 2, ... Fiber n) marked 2, 30 and 32, which are selectively connectable to the optical communication link 16 according to the order set by the key 21. The fiber sections may be manufactured from fibers with different dispersion characteristics (say, among them there may be conventional fiber sections and sections of the DCF fibers). They may have different lengths. According to the key, the sections may be connected to the transmission line in a pseudo-random order and for different time periods thus forming a unique pattern of encryption. The dispersion decryption device suitable to the described encryption device is preferably built based on the same principle,

and, when synchronized with the encryption device, should connect to the transmission line 16 such a fiber section in its module, which would compensate action of the fiber section active in the module of the encryption device at the corresponding moment.

Fig. 4 illustrates how the inventive principle can be implemented in a multi-channel optical transmission system, such as a Wavelength Division Multiplexing system (WDM). The system 40 comprises a transmitting site 42, a receiving site 44 and an optical communication link 46. The transmitting site comprises transmitters 48 (T1, T2,...Tn) of "n" optical information channels each characterized by its particular wavelength. For transmitting information of "n" the optical channels via one common optical fiber communication link 16, the optical signals are multiplexed by the optical multiplexer (MUX) 50. At the receiving site 44, the optical signal from the link 46 is demultiplexed by the demultiplexer (DMUX) 52 , upon which the optical channels are received by their respective receivers 54 (R1, R2, ...Rn).

If the optical communication link comprises an OADM 56 (Optical Add Drop Multiplexer), some of the optical channels are dropped , and some are added between the transmitting site and the receiving site. To protect the information transmitted in any of the optical channels via the link 46, a number of embodiments of the prsent invention can be proposed.

a) each optical channel can be encrypted by its own Dispersion Encryption Device (DED1, DED2, ...DEDn) 58, before being multiplexed at the transmitting site. The encryption keys of different DED 58 may be different. Accordingly, each optical channel can be decrypted at the receiving site by their own Dispersion Decryption Device (DDD1, DDD2,...DDDn) 60. Keys of the respective DED 58 and DDD 60 should correspond to one another and be synchronized.

However, if a particular optical channel (i) is dropped by the OADM 56, an individual DDDi 62 can be provided before the receiver Ri. The DDDi 62 should have the key suitable to the key of the DEDi 58 and be synchronized with it. Likewise, if a particular optical channel (i) is added at the OADM 56 to replace the dropped one, it can be first encrypted by a DEDi' 64, then added to the link 46 and decrypted, upon demultiplexing, by a DDDi 60 at the receiving site. The DDDi 60 and the DEDi' 64 should have a suitable encryption/decryption key and be synchronized.

b) Alternatively, the multi-channel information can be encrypted at the transmitting site by a common DED(T) 66 (shown by dotted lines), and decrypted by a common DDD (R) 68 at the receiving site. If OADM is inserted in the optical communication link, it can be provided with a local DDD(L) 70 at its input, and a local DED(L) 72 at its output. All the devices 66, 68, 70 and 72 may use similar encryption/decryption keys, but should be suitably synchronized. However, the DED 66 and DDD 70, and DED64 and DDD 68 may work in pairs, so that each of the pairs has its own encryption/decryption key.

c) Various combinations of the per-channel encryption described in a) and common encryption described in (b) can be proposed, i.e. the encryption technique may include encryption of both information transmitted via a particular optical channel, and information transmitted over a particular optical fiber.

It should be appreciated that other patterns of the encryption/decryption keys, and other implementations of the dispersion encryption/decryption device can be proposed and should be considered part of the present invention.